IN THE UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

United States of America,)
) Criminal No. 2:15-875-RMG
v.)
) **ORDER**
Jamison Franklin Knowles.)
)

This matter is before the Court on Defendant's motion to suppress evidence (Dkt. No. 47). After careful review of the parties' briefs and following a hearing held on September 6, 2016, the Court denies Defendant's motion.

I. Background

Defendant is charged with possession of child pornography, in violation of 18 U.S.C. § 2252A. The charge arises from the Government's investigation of a website known as "Playpen,"[1] a global forum for distributing child pornography, which used "Tor" software to avoid detection by law enforcement. (Dkt. No. 59 at 1.) Tor prevents tracing internet communications to the actual user. To overcome that obstacle, FBI agents utilized a Network Investigative Technique ("NIT") to identify Playpen users. Using information obtained from the NIT, FBI agents connected Defendant's home address to a Playpen username used to access child pornography. Agents then obtained a warrant to search Defendant's home, wherein they seized computer media containing child pornography. Defendant now moves to suppress those items, arguing the Government's use of an NIT, which was authorized by a search warrant issued in the Eastern District of Virginia, to obtain information from Defendant's computer, which was located

[1] The applications attached as exhibits to the motion to suppress redact the name Playpen as "TARGET WEBSITE" or "WEBSITE A." In this Order, quotations from those applications substitute "Playpen" for "TARGET WEBSITE" or "WEBSITE A."

in South Carolina, violated the Fourth Amendment, Rule 41(b) of the Federal Rules of Criminal Procedure, and 28 U.S.C. § 636(a).

A. Internet Background

Defendant's challenge to the use of an NIT raises issues requiring some background on communications between a website and its users.[2] Websites exist on computers called "servers." A computer accessing the website is a "client" computer. Website servers and their clients typically are not part of the same home or office computer network. Thus, communications between server and client require a connection between networks—a means of "internetworking" (hence, the "internet"). This is accomplished by assigning internet protocol ("IP") addresses, bundling communications into data "packets" bearing source and destination IP addresses, and using specialized devices, "network nodes," to forward the data packets between networks. Each data packet has a "header" containing the source IP address, the destination IP address, and other data needed to route the packet. Network nodes use those IP addresses to route the packet between the user's location and the website's location, which might be the other side of the world.

The process may be analogized to physical mail. Communications are bundled into an envelope or "packet," having a "header" with source and destination addresses. The packet is forwarded among various "nodes," post offices and mail distribution centers, resulting, ultimately, in delivery to the intended recipient. By that analogy, to interact with a website is to engage in a correspondence with it. A closer analogy may be correspondence via telephone text messaging—an exchange of short messages across a communications network between persons using devices associated with unique numbers. The text message analogy illustrates IP addresses are subscriber

[2] For an overview of internet communications and bibliography, *see generally, e.g.*, Kevin Werbach, *The Centripetal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. Davis L. Rev. 343 (2008).

numbers assigned by a service provider, like a telephone number, and not physical locations, like a mailing address. An internet service provider can provide subscriber information, including location information, regarding IP addresses, just as a telephone service provider may provide subscriber information regarding telephone numbers. (*See* Dkt. No. 47-1 ¶ 22.) The service provider responsible for a given IP address may be identified using publicly available information, again, just as a telephone company may be identified for a given telephone number. (*Id.*)

Finally, not all network addresses are used to route communications across the internet. Some addresses are local addresses valid for communications only within a single network or portion of a network. *See* Barrie Sosinsky, *Networking Bible* 512–13 (2009); Jielin Dong, *Network Dictionary* 298 (2007); Richard E. Smith, *Elementary Information Security* 509–10 (2001). Network nodes do not forward packets with such addresses between networks. *How to Accelerate Your Internet: A Practical Guide to Bandwidth Management and Optimisation Using Open Source Software* 45 (Rob Flickenger, ed., 2006). These addresses again can be analogized with telephones, as number extensions on a shared line—persons in the same office can reach one another by dialing an extension, but outside persons must dial the number for main line and all outgoing calls display that number on "caller ID."

A media access control address ("MAC address") is a type of local address at issue in this case. A MAC address is assigned to a network interface, usually by the manufacturer, to identify devices on a network. Smith, *supra*, at 462–63; *see also Azure Networks, LLC v. CSR PLC*, 771 F.3d 1336, 1347 (Fed. Cir. 2014) (discussing MAC addresses), *judgment vacated on other grounds*, 135 S. Ct. 1846 (2015). In practice, this means a computer has a MAC address analogous to an automobile's Vehicle Identification Number.[3] *See United States v. Cone*, 714 F.3d 197, 210 n.9 (4th Cir. 2013). MAC addresses generally not transmitted over the internet, and websites generally cannot request (or "instruct") a client to transmit its MAC address directly. Flickenger, *supra*, at 45. To obtain a client's MAC address, a website must somehow bypass the client's normal security measures.

B. The Tor Network

Normally, law enforcement can review a website's IP address logs after they seize a website to determine which IP addresses visited the site. (*See* Dkt. No. 47-1 ¶ 22.) They can then search public information to determine which internet service provider owned a target IP address and issue a subpoena to that service provider for the identity of the user of that IP address. (*Id.*) Playpen users, however, concealed their IP addresses with Tor. (Dkt. No. 47-3 ¶ 7.) The Department of Defense designed Tor to protect government communications, but it is now free software available to the public. (*Id.*) The NIT search warrant affidavit describes Tor as masking users' IP addresses by "bouncing their communications around a distributed network of relay computers run by volunteers all around the world." (*Id.* ¶ 8.) However, "bouncing . . . communications around a distributed network . . . all around the world" describes most internet communications. More specifically, Tor utilizes "onion routing" to make internet communications anonymous. (Tor is an acronym for "The Onion Router.")[4] In onion routing, packets are the core of layered cells or "onions." Around that core are layers of encryption. Special software on the

[3] A computer may have multiple MAC addresses, *e.g.*, one for a wireless network adapter and one for an Ethernet adapter. A computer's MAC address may be changed by replacing a network adapter or by other means not relevant here.

[4] For a detailed description of Tor and onion routing, *see generally* Rodger Dingledine, Nick Mathewson, & Paul Syverson, *Tor: The Second-Generation Onion Router*, *available at* https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf. *See also* Tor Documentation, The Tor Project, Inc., https://www.torproject.org/docs/documentation.html.en

user's computer chooses a "circuit" through the network of Tor servers, known as "onion routers." There are approximately seven thousand publicly listed routers and another two thousand unlisted routers (used to prevent service providers from blocking access to the Tor network). *See* Tor Metrics, The Tor Project, Inc., https://metrics.torproject.org/networksize.html. Each onion router decrypts a layer of the onion, receiving instruction on where next to relay it. No onion router knows how many routers are in the circuit, and only the last router in the circuit, the "exit node," knows its position in the circuit. When the onion leaves the exit node, it proceeds to its destination as any other internet traffic, but with the exit node's IP address rather than the actual sender's IP address.

Onion routing may be analogized with the following example. John receives a locked box, for which he has the key. He opens it, finding within another locked box, labeled "Jane." He does not have the key for Jane's box, so he mails the box to Jane. Jane has the key, and within she finds a locked box labeled "Jack." She does not have the key for Jack's box, so she mails it to Jack. Jack likewise opens his box, finds within a locked box labeled "Jill," and mails that box to Jill. Jill opens her box to find an envelope bearing a website's address. She writes her own address as the return address and mails the letter. This process is reversible, so information from a website can return through the Tor network to the end user. But it is impossible for the website to identify the actual IP address of the end user. Nor does John, Jane, Jack, or Jill know who is communicating with whom. As a result, "traditional IP identification techniques are not viable" because the last computer or exit node is not the IP address of the actual user who visits the website. (Dkt. No. 47-3 ¶ 8.) It is impossible to trace the exit node's IP address to the originating computer. (*Id.*)

Tor also allows websites, such as Playpen, to operate as a "hidden service." (*Id.* ¶¶ 9–10.) Tor replaces the website server's IP address with a Tor web address. (*Id.* ¶ 9.) The Tor web address "is a series of algorithm-generated characters, such as 'asdlk8fs9dflku7f' followed by the suffix '.onion.'" (*Id.*) Users had to obtain Playpen's specific address from other users or through a link posted on one of Tor's "hidden services" pages dedicated to child pornography. (*Id.* ¶ 10.)

C. Playpen

Playpen needed the anonymity Tor provides because it was "dedicated to the advertisement and distribution of child pornography, [and] the discussion of matters pertinent to child sexual abuse." (*Id.* ¶ 6.) The website's home page displayed an image of two partially clothed prepubescent females with their legs spread apart. (*Id.* ¶ 12.) That page prompted users either to register an account or to login using an existing username and password. (*Id.*) A message told registering users "NOT [to] . . . enter a real [email] address" and "[f]or your security you should not post information here that can be used to identify you." (*Id.* ¶ 13.) The message also stated, "This website is not able to see your IP address and can not [*sic*] collect or send any other form of information to your computer except what you expressly upload." (*Id.*)

After logging in, users saw a page listing discussion boards for images, videos, or text related to child pornography, including "Preteen Photos," "Pre-teen Videos," "Pre-Teen Photos," "Family – Incest" and "Toddlers." (*Id.* ¶ 14.) Within the pre-teen videos and photos discussion boards were "subforums" titled "Girls [hardcore]," "Boys [hardcore]," "Girls [softcore/non-nude]" and "Boys [softcore/non-nude]." (*Id.*) Playpen also included features called "Playpen Image Hosting" and "Playpen Video Hosting," which allowed users to upload images and videos of child pornography for other users to view. (*Id.* ¶ 23.) Over 1,500 unique users visited Playpen daily and over 11,000 unique users visited the site over the course of a week. (*Id.* ¶ 19.) By March 2015, Playpen contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members. (Dkt. No. 47-1 ¶ 12.)

In December 2014, a foreign law enforcement agency informed the FBI it suspected a United States-based IP address was associated with Playpen. (Dkt. No. 47-3 ¶ 28.) The FBI determined the subject IP address was owned by a server hosting company headquartered in North Carolina.[5] (*Id.*; Dkt. No. 59 at 2.) The FBI subsequently obtained a search warrant for the server. (Dkt. No. 47-3 ¶ 28.) FBI agents examined the server and determined it contained a copy of Playpen. They then stored the copy of the website on a computer server at a government facility in Newington, Virginia. Newington is located in the Eastern District of Virginia. (*Id.*) Additional investigation revealed a Florida resident controlled Playpen. (*Id.*) On February 19, 2015, FBI personnel executed a court-authorized search of the administrator's residence in Florida. (*Id.* ¶ 30.) The FBI arrested the suspect and assumed control of Playpen. (*Id.*)

D. The Network Investigative Technique

On February 20, 2015, Special Agent Douglas Macfarlane applied to a United States Magistrate Judge in the Eastern District of Virginia for a search warrant to use an NIT with Playpen (the "NIT search warrant"). (*See generally* Dkt. No. 47-3.) In the warrant application, Agent Macfarlane stated the NIT was necessary to overcome the anonymity Tor provides. (*Id.* ¶ 31.) The NIT would "augment" the normal content Playpen sends to users with "additional computer instructions" that "are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government." (*Id.* ¶ 33 & p.37.) That information comprised (1) the user's IP address, (2) the operating system running on the user's computer (*e.g.*, Windows 7), (3) the user's computer's network name, (4) the user's computer's operating system username, (5) MAC addresses associated with the user's computer, (6)

[5] A server hosting company leases space for a server, and sometimes the server hardware itself, within a data center.

"Information about whether the NIT has already been delivered to the 'activating' computer,"[6] and (7) a unique identifier generated by the NIT to distinguish data from the computer from data sent by other computers connecting to Playpen. (*Id.* ¶ 34.) The warrant application sought operating system, computer name, and MAC address information to enable identification of a specific computer within a household sharing an IP address, and possibly identification of a specific user of a shared computer. Hr'g Tr. 27:19–30:11, *United States v. Matish*, Crim. No. 4:16-16 (E.D. Va. May 19, 2016), Dkt. No. 61.

The warrant provided that the NIT would activate "each time that any user or administrator log[ged] into Playpen by entering a username and password." (Dkt. No. 47-3 ¶ 36.) However, in practice the FBI configured the NIT to activate only when a user accessed certain posts within Playpen. Hr'g Tr. 20:19–25, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 ("The way you deployed it is much narrower than what the warrant authorized, correct? [Agent Alfin answering] That is correct."). The NIT did not activate when a user reached Playpen's home page, created an account, or logged into that account. Hr'g Tr. 69:19–21, *United States v. Michaud*, Crim. No. 15-5351 (W.D. Wash. Jan. 22, 2016), Dkt. No. 203 ("THE COURT: The NIT did not just go to anyone that logged into the website? THE WITNESS [Agent Alfin]: No, your Honor. The warrant did authorize us to deploy the NIT in that fashion. [But it allowed the FBI to] restrict how we deploy the NIT, [so we] deployed it in such a fashion that the NIT was deployed against users who attempted to access illicit content."). To activate the NIT, a user actually had to access child

[6] The meaning of this is unclear. Because the NIT is sending the data, it obviously "has already been delivered." This may mean the NIT can determine whether it was previously deployed to a user's computer. However, FBI Special Agent Daniel Alfin has testified the NIT leaves no trace of itself on target computers. Hr'g Tr. 22:3–6, *United States v. Matish*, Crim. No. 4:16-16 (E.D. Va. May 19, 2016), Dkt. No. 61; Hr'g Tr. 19:21–20:1, *Matish*, Crim. No. 4:16-16 (E.D. Va. June 14, 2016), Dkt. No. 86.

pornography. *See, e.g.*, Hr'g Tr. 27:19–30:11, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 (FBI Agent Alfin testifying the NIT only deployed when the defendant in that case sought images of bestiality involving an eleven year-old girl); Hr'g Tr. 69:8–16, *Michaud*, Crim. No. 15-5351, Dkt. No. 203 (FBI Agent Alfin testifying the NIT only deployed when the defendant in that case sought images contained in a portion of Playpen entitled "Preteen Videos—Girls Hardcore" because "[a]t the point where a user in that forum accessed a post, we can affirmatively state that a user has attempted to access child pornography"). Once activated, the NIT caused the "activating computer—wherever located—to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer." (Dkt. No. 47-3 ¶ 46.) The FBI could then link a username and its corresponding activity on the site with an IP address. (*Id.* ¶ 37.) As explained above, IP addresses can be used to determine location, and other information gathered by the NIT, such as a local computer account name and MAC address, can link a particular computer found at a location to a Playpen user.

The NIT consists of four parts: (1) computer code on Playpen, which associates Playpen usernames with the unique identifier generated by the NIT; (2) an "exploit," computer code taking advantage of a security flaw in the user's computer to enable the FBI's "additional computer instructions" to execute surreptitiously on the user's computer; (3) the "additional computer instructions" surreptitiously executed on the user's computer to find the information to be seized and to transmit it to the FBI; and (4) a separate FBI-controlled computer, which receives the information the NIT transmits from users' computers. Decl. of Vlad Tsyrklevich ¶¶ 4, 6, *Matish*, Crim. No. 4:16-16 (June 23, 2016), Dkt. No. 37-1 (prepared for the defense in *Michaud*, Crim. No. 15-5351, and referenced in the Alfin Declaration filed by Defendant, Dkt. No. 58-1 ¶ 5); *see also*

Hr'g Tr. 18:6–24, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 (FBI Agent Alfin testifying the NIT's "supplemental instructions" "downloads" to a user's computer, "wherever it may be located," and the "downloading is intended not to be observed by the user"); Hr'g Tr. 77:11–16, *Michaud*, Crim. No. 15-5351, Dkt. No. 203 (FBI Agent Alfin testifying the NIT was "intended to be invisible to the user"). After transmitting information to the FBI, the NIT removed itself from the user's computer. Hr'g Tr. 22:3–6, *Matish*, Crim. No. 4:16-16, Dkt. No. 61; Hr'g Tr. 19:21–20:1, *Matish*, Crim. No. 4:16-16, Dkt. No. 86.

In Attachment A to the warrant application, which identified the "place to be searched," Agent Macfarlane stated the NIT would be "deployed on the computer server . . . located at a government facility in the Eastern District of Virginia." (Dkt. No. 47-3 at 36.) Agent Macfarlane knew the NIT would deploy to computers outside the Eastern District of Virginia. Hr'g Tr. 64:15–65:19, *Matish*, Crim. No. 4:16-16, Dkt. No. 61. He believed Rule 41(b)(4) of the Federal Rules of Criminal Procedure nonetheless authorized the warrant, on the theory Playpen users' computers "virtually" entered the Eastern District of Virginia when they communicated with Playpen and the NIT was a tracking device installed on computers while they were "virtually" in the Eastern District of Virginia. Hr'g Tr. 64:20–65:20, *Matish*, Crim. No. 4:16-16, Dkt. No. 61 (Agent Macfarlane testifying to his understanding the NIT warrant fell under the "tracking device" provision of Rule 41(b)(4)).

On February 20, 2015, the magistrate judge issued the search warrant. (Dkt. No. 47-3 at 2.) The Government also applied for and received an order authorizing interception of electronic communications pursuant to 18 U.S.C. § 2518 (the "Title III order"), to allow interception of electronic communications occurring over Playpen's private messaging and chat functions. (Dkt. No. 47-2.) The FBI thereafter operated Playpen until March 4, 2015. (Dkt. No. 47 at 1.) The investigation over that two-week period resulted in charges against at least 137 persons, including 35 child molesters and 17 producers of child pornography, and the identification or recovery of at least 26 child victims. United States' Response to Order Compelling Discovery 7–8, *Michaud*, Crim. No. 15-5351 (Jan. 8, 2016), Dkt. No. 109.

E. Identification of Defendant

According to Playpen's logs and information obtained from the NIT, a user with username "min878" registered for a Playpen account on January 14, 2015. (Dkt. No. 47-1 ¶¶ 25–26.) He engaged in the following activity from IP address 66.56.186.156:

- On February 28, 2015, he accessed images of "a pre-pubescent female, nude from the waist down, legs spread apart with the focus on her vaginal area." (*Id.* ¶ 28.)
- On March 1, 2015, he accessed images of "a pre-pubescent female being anally penetrated by a vibrator and an adult male's penis." (*Id.* ¶ 30.)
- On March 4, 2015, he accessed more images of a pre-pubescent female's vagina. (*Id.* ¶ 31.)

The FBI determined from public information that Time Warner Cable owned IP address 66.56.186.156. (*Id.* ¶¶ 32–33.) The FBI served an administrative subpoena on Time Warner Cable in March 2015, requesting information related to the user assigned that IP address. (*Id.* ¶ 33.) Information received from Time Warner Cable enabled the FBI to determine IP address 66.56.186.156 was assigned to Kenneth Knowles (Defendant's father). (Dkt. No. 47 at 4; Dkt. No. 47-1 ¶¶ 33–37.) The FBI obtained a search warrant for Mr. Knowles residence on November 4, 2015; the warrant was executed on November 10, 2015. (Dkt. No. 47 at 4.) Agents seized personal computers and other digital devices containing child pornography. (*Id.*)

F. Procedural History

On December 8, 2015, Defendant was indicted for possession of child pornography involving a prepubescent minor. (Dkt. No. 1.) On August 18, 2016, Defendant moved to suppress evidence seized pursuant to the search warrant of February 20, 2015, which authorized use of the NIT. (Dkt. No. 47.) The Court held a hearing on the motion on September 6, 2016. On September 8, 2016, Defendant filed a supplemental motion to suppress. (Dkt. No. 58.) That supplemental motion includes as Part I "Supplemental Factual Information" regarding the motion to suppress *sub judice*, and as Part II "Additional Grounds for Suppression," a separate motion seeking, pursuant to *Miranda v. Arizona*, 384 U.S. 436 (1966), to suppress statements Defendant made to investigators. This Order does not address Defendant's *Miranda* claims.

II. Legal Standard

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. All warrants must "(1) be issued by a neutral and detached magistrate, (2) contain a particular description of the place to be searched, and the person or things to be seized, and (3) be based upon probable cause, supported by Oath or affirmation." *United States v. Clyburn*, 24 F.3d 613, 617 (4th Cir. 1994). Evidence seized pursuant to a warrant lacking one of those requirements may be suppressed. However, "[s]uppression of evidence . . . has always been [the court's] last resort, not [the court's] first impulse." *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Because the consequences of suppression are dire, a defendant urging suppression carries a heavy burden. *See id.* Suppression is limited to cases in which its deterrent effect against law enforcement's misconduct outweighs the costs inherent in barring evidence that law enforcement expended great resources to obtain. *See Penn. Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 357 (1998) (citing *United States v. Leon*, 468 U.S. 897, 907 (1984)).

Magistrate judges usually issue search warrants. Their authority originates in the Federal Magistrates Act, which in relevant part it provides,

> (a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> > (1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts;

28 U.S.C. § 636(a). Rule 41(b) of the Federal Rules of Criminal Procedure, incorporated by the Federal Magistrates Act in the above text, provides

> (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:
>
> > (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
> >
> > (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
> >
> > (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
> >
> > (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
> >
> > (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
> >
> > > (A) a United States territory, possession, or commonwealth;

> (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

"Although the purpose of Rule 41 is the implementation of the [F]ourth [A]mendment, the particular procedures it mandates are not necessarily part of the [F]ourth [A]mendment." *United States v. Searp*, 586 F.2d 1117, 1121 (6th Cir. 1978). A constitutionally reasonable search may violate the procedural requirements of Rule 41. *Id.* at 1122. The Fourth Circuit therefore distinguishes between two types of Rule 41 violations: those that involve the constitutional violations and those that do not. *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000). Suppression is warranted for non-constitutional violations of Rule 41 "only when the defendant is prejudiced by the violation or when there is evidence of intentional and deliberate disregard of a provision in the Rule." *Id.* (internal citations and quotations omitted).

III. Discussion

Defendant argues the NIT search warrant does not contain a particular description of the place to be searched, because the location of Defendant's computer was unknown when the warrant issued, and so violates the Fourth Amendment. (Dkt. No. 47 at 13–14.) Defendant also argues the NIT search warrant's issuance in Virginia violates Rule 41(d) in a manner requiring suppression, (1) because it was void *ab initio* because it exceeded the magistrate judge's authority under the Federal Magistrates Act, (2) because the violation prejudiced Defendant, and/or (3) because law enforcement acted in bad faith or with deliberate disregard of Rule 41 when obtaining the warrant. (*Id.* 5–11.) He moves to suppress evidence seized from his home, because the probable cause supporting the warrant for that search was a fruit of the NIT search warrant.

Many federal courts have addressed the NIT search warrant at issue here. Courts generally find the magistrate judge in Virginia lacked authority to issue the NIT search warrant without finding suppression to be appropriate. *See, e.g.*, *United States v. Henderson*, Crim. No. 15-565, 2016 WL 4549108 (N.D. Cal. Sept. 1, 2016) (denying motion to suppress); *United States v. Adams*, Crim. No. 6:16-11, 2016 WL 4212079 (M.D. Fla. Aug. 10, 2016) (same); *United States v. Acevedo-Lemus*, Crim. No. 15-137, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016) (same); *United States v. Eure*, Crim. No. 2:16-43, 2016 WL 4059663 (E.D. Va. July 28, 2016) (same); *United States v. Matish*, Crim. No. 4:16-16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Darby*, Crim. No. 2:16-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (same); *United States v. Werdene*, Crim. No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (same); *United States v. Epich*, Crim. No. 15-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016) (same); *United States v. Stamper*, Crim. No. 1:15-109 (S.D. Ohio, Feb. 19, 2016) (same); *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (same); *but see also, e.g.*, *United States v. Arterbury*, slip op., Crim. No. 15-182 (N.D. Okla. May 12, 2016) (granting motion to suppress), *appeal docketed*, No. 16-5117 (10th Cir. July 27, 2016); *United States v. Levin*, Crim. No. 15-10271, 2016 WL 2596010 (D. Mass. May 5, 2016) (same), *appeal docketed*, No. 16-157 (1st Cir. May 20, 2016).

A. The NIT Performed a Search

A Fourth Amendment search occurs when "the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979). There are two components to a reasonable expectation of privacy: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Defendant claims the NIT violated his Fourth Amendment rights. He must therefore demonstrate that the NIT violated a subjective expectation of privacy and that society is prepared to recognize that expectation as reasonable. *Smith*, 442 U.S. at 740.

The NIT retrieved several types of information from Defendant's computer. (*See* Dkt. No. 47-3 ¶¶ 34.) The most important information retrieved from Defendant's computer was his IP address, which informed authorities of Defendant's location and led to the search that Defendant wishes suppressed. The government contends Defendant had no reasonable expectation of privacy in his IP address. (Dkt. No. 59 at 14–15.) Courts uniformly hold there is no reasonable expectation of privacy in an IP address, a number assigned Defendant by his service provider, which he voluntarily provided to third parties every time he used the internet. *See Henderson*, 2016 WL 4549108, at *5; *Adams*, 2016 WL 4212079, at *4; *Acevedo-Lemus*, 2016 WL 4208436, at *4; *United States v. Laurita*, Crim. No. 8:13-107, 2016 WL 4179365, at *5 (D. Neb. Aug. 5, 2016); *Matish*, 2016 WL 3545776, at *21; *Werdene*, 2016 WL 3002376, at *10; *Michaud*, 2016 WL 337263, at *7; *see also United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) ("'[E]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'" (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008))). But the IP address was not the only information the NIT retrieved from Defendant's computer. It also retrieved his MAC address, local computer operating system information, and local compute operating system login username. (Dkt. No. 47-3 ¶ 34.) The Government needed that information to identify Defendant as the person accessing Playpen under the user name mim878. *See* Hr'g Tr. 27:19–30:11, *Matish*, Crim. No. 4:16-16, Dkt. No. 61. To obtain that information, the NIT surreptitiously placed code on Defendant's personal computer that extracted the information. (*See* Dkt. No. 47-3 ¶¶ 33–34.) Thus, the relevant inquiry is whether Defendant has a reasonable expectation of privacy in the contents of his personal computer, which was located in his home, not whether he has a reasonable expectation of privacy in his IP address.

Individuals generally have a reasonable expectation of privacy in the contents of their home computers. *See United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (finding reasonable expectation of privacy in password-protected files on a computer); *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside the home."). The Court is aware of no authority holding persons have no reasonable expectation of privacy in their personal computers located within their homes. Moreover, as the *Darby* court observed when denying a suppression motion in another criminal prosecution arising from the Playpen investigation: "The prohibition against hacking is itself proof of society's acceptance of the privacy expectations of personal computer users." 2016 WL 3189703, at *5–6 (citing 18 U.S.C. § 1030(a)(2)(C)).

The NIT "downloaded" surreptitiously to Defendant's computer to search his computer for personally identifying information not routinely disclosed over the internet. That is a search within the meaning of the Fourth Amendment. As the *Darby* court held,

> Likewise, if an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search. The NIT in this case caused Defendant's computer to download certain code without the authorization or knowledge of Defendant. . . . [T]he code placed on Defendant's computer caused Defendant's computer to transmit certain information without the authority or knowledge of Defendant. In this manner the government seized the contents of Defendant's computer.

2016 WL 3189703, at *6. The Court agrees with that analysis. Some courts, however, have held even the retrieval of Defendant's IP address falls within the Fourth Amendment's ambit, because it was obtained by searching a constitutionally protected area. For example, the *Adams* court observed,

> There is little doubt that had law enforcement officers obtained Defendant's IP address from a non-Tor-based server and issued a subpoena to the ISP to determine Defendant's physical address, a motion to suppress the information obtained from the ISP would be without merit. However, Defendant's IP address was discovered only after property residing within Defendant's home—his computer—was searched by the NIT.

2016 WL 4212079, at *4. Likewise, the *Darby* court held, "It was irrelevant that the individual might not have a reasonable expectation of privacy in the information actually obtained." 2016 WL 3189703, at *6. This Court cannot agree with that reasoning. The Supreme Court has held "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351. IP addresses are knowingly exposed to the public; they therefore are not subject to Fourth Amendment protection. However, in this case the Government obtained information subject to Fourth Amendment protection to identify the user of Playpen account min878 as Defendant, rather than, for example, Defendant's father, who was the account holder for the IP address. The Court therefore finds the government's deployment of the NIT unto Defendant's computer was a Fourth Amendment search.

B. The Warrant Violated Rule 41

Defendant argues that under Rule 41(b), a magistrate judge's authority to issue a search warrant is limited to her own judicial district except in certain circumstances that do not exist in this case. Therefore, according to Defendant, Rule 41(b) did not authorize issuance of the NIT search warrant, and the NIT performed a warrantless search violative of the Fourth Amendment. The Government argues the NIT search warrant was valid under Rule 41(b)(1), (2), and (4) because the Playpen server was located in the Eastern District of Virginia and Playpen users had to reach virtually into the Eastern District of Virginia to access Playpen, at which time the NIT was installed on their computers. (Dkt. No. 59 at 6–8.)

The NIT search warrant plainly was impermissible under Rule 41(b)(1) and (2). Those sections allow a magistrate judge to issue a warrant to search property located within the magistrate judge's district, presently or at the time when the warrant is issued. Neither applies here because the NIT searched a computer in South Carolina, which was never located within the Eastern District of Virginia. The Government argues Defendant's computer was somehow actually in the Eastern District of Virginia for purposes of Rule 41(b) because it "reached into [the Eastern District of Virginia's] jurisdiction to access" Playpen. (Dkt. No. 59 at 7.) That argument is unpersuasive. As explained above, to access a website is, essentially, to correspond with it. The Government's argument would make a cell phone "property located within the district" when it exchanges text messages with someone located within that district. Moreover, even if the Government's reasoning were accepted, Defendant's computer was "in" the Eastern District of Virginia only when it accessed Playpen. When the warrant issued, Defendant's computer was outside the district and not accessing Playpen. *Cf.* Fed. R. Crim. P. 41(b)(2) (providing "a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district *when the warrant is issued* (emphasis added)).

Rule 41(b)(4), which authorizes a magistrate judge "to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both," also is inapposite. The Eastern District of Virginia has found the NIT search warrant permissible under Rule 41(b)(4) because it allowed the FBI to install a tracking device on the computers of Playpen users when those computers "digitally touched down in the Eastern District of Virginia when they logged into the site." *Darby*, 2016 WL 3189703, at *12. Jun. 3, 2016); *see also United States v. Matish*, No. 16-cr-16, 2016 WL 3545776 (E.D. Va. Jun. 23, 2016). The Government similarly argues the NIT was "an electronic . . . device which permits the tracking of . . . a person." (Dkt. No. 59 at 6.) Most courts, however, have found that argument unpersuasive. "The NIT search does not meet the requirements of 41(b)(4) because, even though it was analogous to a tracking device in some ways, it nevertheless falls outside the meaning of a 'tracking device' as contemplated by the rule. Further, the NIT was installed outside of the district, at the location of the activating computers, not within the district as required by Rule 41(b)(4)." *Henderson*, 2016 WL 4549108, at *4. The "NIT does not track; it searches." *Adams*, 2016 WL 4212079, at *6. Rule 41(b)(4) is "premised on the person or property being located within the district. It is uncontested the computer information the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia." *Werdene*, 2016 WL 3002376, at *7; *see also Michaud*, 2016 WL 337263, at *6 ("[A]pplying subdivision (b)(4), which allows for tracking devices installed within one district to travel to another, stretches the rule too far."). This Court agrees the NIT does not meet the requirements of 41(b)(4) because it was installed outside of the Eastern District of Virginia to search Defendant's computer for information never present in the Eastern District of Virginia.

Rule 41 is read flexibly. *See United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977). "Even a flexible application of the Rule, however, is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections." *Werdene*, 2016 WL 3002376. In this case, the NIT search warrant was not permissible under any of the five subsections of Rule 41(b) because it was issued by a magistrate judge in the Eastern District of Virginia yet permitted searches of Defendant's computer, which at all relevant times was in South Carolina.

C. Suppression is Inappropriate

Rule 41 violations are either constitutional violations or non-constitutional violations. *Simons*, 206 F.3d 392, 403. A constitutional violation may result in suppression, if no exception to suppression applies. But suppression is justified for a non-constitutional violation of Rule 41 only when the defendant is prejudiced or when there is intentional and deliberate disregard of the rule. *Id.*

The Court finds suppression of the fruits of the NIT search warrant inappropriate for several separate and independent reasons. The search warrant was not void *ab initio*, as Defendant argues. Rather, it was a valid search warrant, at least in the Eastern District of Virginia, that satisfied all Fourth Amendment requirements. Even if that were not the case, the Government relied upon its validity in good faith. Even if the Government had learned Defendant was in South Carolina, exigent circumstances would have justified the NIT search without first obtaining a warrant in South Carolina. Finally, the ministerial violation of Rule 41 that occurred in this case does not justify the exclusion of evidence seized on probable cause and with advance judicial approval, because the Government did not intentionally disregard the rule and because the violation did not prejudice Defendant.

1. The Warrant Was Not Void *Ab Initio*

The NIT performed a search of Defendant's computer, within the meaning of the Fourth Amendment, and the magistrate judge lacked authority under Rule 41 to authorize that search. Defendant argues that defect renders the NIT search warrant void *ab initio*, as if it had never been signed at all, making the search of his computer a constitutional violation—a warrantless search in violation of the Fourth Amendment. (Dkt. No. 47 at 8.) Defendant's argument relies principally on *Levin*, which "there was simply no judicial approval" for the NIT search warrant "because the magistrate judge lacked authority, and thus jurisdiction, to issue" it. *Levin*, 2016 WL 2596010, at *8.

The Court cannot agree there was "no judicial approval" for the NIT search warrant, thereby rendering it void *ab initio*, because Magistrate Judge Theresa Buchanan approved the warrant. (Dkt. No. 47-3 at 38.) The Supreme Court has made clear

> [t]he substance of the Constitution's warrant requirements does not turn on the labeling of the issuing party. The warrant traditionally has represented an independent assurance that a search and arrest will not proceed without probable cause to believe that a crime has been committed and that the person or place named in the warrant is involved in the crime. Thus, an issuing magistrate must meet two tests. He must be neutral and detached, and he must be capable of determining whether probable cause exists for the requested arrest or search.

Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972). Because Magistrate Judge Buchanan was a neutral and detached judicial officer, authorized to issue search warrants and capable of determining whether probable cause existed, her approval of the search warrant was constitutionally sufficient judicial approval. Moreover, Rule 41(b) authorized her to issue the NIT search warrant for the search of Playpen users located within the Eastern District of Virginia or within territorial, diplomatic, or consular areas outside any judicial district. *See* Fed. R. Crim. P. 41(b)(1), (5). The Rule 41 violation with regard to Defendant merely was approval by a neutral and detached magistrate other than the one specified by the Federal Rules of Criminal Procedure.

2. The Warrant Satisfied the Fourth Amendment

The NIT search warrant complied with the Fourth Amendment's requirements of probable cause and particularity. *See* U.S. Const. amend. IV (providing "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"). The application for the NIT search warrant provided substantial probable cause for the warrant to issue by describing overwhelming evidence Playpen was used to host and exchange child pornography. All courts analyzing the NIT search warrant have found it supported by probable cause. *See, e.g.*, *Henderson*, 2016 WL 4549108, at *4, *Darby*, 2016 WL 3189703, at *8; *Michaud*, 2016 WL 337263, at *8. Defendant has not challenged the probable cause supporting the warrant.

Defendant's constitutional challenge to the NIT search warrant is that it "failed to comply with the Fourth Amendment's particularity requirements." (Dkt. No. 47 at 13.) The Court finds no merit in that argument. As the *Henderson* court observed, the warrant provides the NIT will

> obtain[ ] information . . . from the activating computers," that are "those of any user or administrator who logs onto [Playpen] by entering a username and password." NIT Warrant, Attachment A. This description is sufficiently particular because it is limited only to individuals that log onto the Playpen website using a username and password. Because of the structure of the Tor network, only individuals actively attempting to access the Playpen website, with sufficient knowledge of the website and its contents, are able to access it. The Warrant is sufficiently particular as it specifies that the NIT search applies only to computers of users accessing the website, a group that is necessarily actively attempting to access child pornography.

2016 WL 4549108, at *4. This Court agrees: A search warrant seeking an address from any computer that deliberately logs into a hidden, illegal website hosted on a particular server is sufficiently particular, despite Defendant's argument that "[h]ad the government particularly described the place to be searched, *i.e.*, a computer in South Carolina, no warrant could have issued." (Dkt. No. 47 at 13.) Defendant's argument is tendentious. The point of the NIT search warrant was to learn the location of computers accessing Playpen. If the Government knew Defendant's computer was in South Carolina, no NIT search warrant regarding this Defendant would have issued because the Government would not have needed one. Moreover, the Supreme Court has squarely rejected Defendant's argument:

> We are also unpersuaded by the argument that a warrant should not be required because of the difficulty in satisfying the particularity requirement of the Fourth Amendment. The Government contends that it would be impossible to describe the "place" to be searched, because the location of the place is precisely what is sought to be discovered through the search. However true that may be, it will still be possible to describe the object into which the beeper is to be placed, the

> circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.

United States v. Karo, 468 U.S. 705, 718 (1984). Here, the Government described the object into which the NIT was to be placed (user computers logging into Playpen), the circumstances that led agents to wish to install the NIT (users accessing child pornography on a hidden website, using advanced encryption tools impervious to normal investigative techniques), and the period of surveillance (the warrant application specified thirty days (Dkt. No. 47-3 at 36), though the operation lasted only two weeks). The Government provided everything necessary "to permit issuance of a warrant authorizing [NIT] installation and surveillance." *See Karo*, 468 U.S. at 718.

3. The Government Relied on the Warrant in Good Faith

Even if the NIT search warrant were somehow deficient under the Fourth Amendment, suppression would not be appropriate because the Government relied upon it in good faith. Suppression is unjustified "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful." *Davis v. United States*, 564 U.S. 229, 238 (2011); *see also Leon*, 468 U.S. at 922 ("[O]bjectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion."). The Government's reliance on the NIT search warrant was objectively reasonable because the warrant "was supported by substantial probable cause, was sufficiently particular in describing the people and places to be searched, and was issued by a neutral magistrate judge." *Henderson*, 2016 WL 4549108, at *6. The exclusionary rule is designed to deter "'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights" by police. *Davis*, 564 U.S. at 238. Here, the Government "presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted." *Werdene*, 2016 WL 3002376, at *15. The issuing magistrate judge was a neutral and detached magistrate with authority to issue search warrants. The Government's application demonstrated ample probable cause and was sufficiently particular. The only error in this case was the "magistrate judge's mistaken belief that she had jurisdiction." *Id.* That mistake cannot justify suppression because "the exclusionary rule is designed to deter police misconduct rather than to punish the errors of judges and magistrates," *Leon*, 468 U.S. at 916.

Defendant's allegation that the Government requested the NIT search warrant in bad faith, and thereby misled the magistrate judge into issuing it, is baseless, and it was well addressed by the *Darby* Court:

> The FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed. The information gathered by the warrant was limited: primarily the IP addresses of those that accessed Playpen and additional information that would aid in identifying what computer accessed the site and what individual used that computer. Defendant seeks suppression because of an alleged violation of a Federal Rule of Criminal Procedure, a rule that will likely be changed to allow explicitly this type of search. The pending amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes. That is, there is nothing unreasonable about the scope of the warrant itself. The FBI should be applauded for its actions in this case.

2016 WL 3189703, at *13.

4. Exigent Circumstances Justified Use of the NIT

Although the Fourth Amendment does not specify when a search warrant must be obtained, the Supreme Court holds "[i]t is a 'basic principle of Fourth Amendment law . . . that searches and seizures inside a home without a warrant are presumptively unreasonable." *Kentucky v. King*, 563 U.S. 452, 459 (2011) (internal quotation marks omitted). That "presumption may be overcome in some circumstances . . . because [t]he ultimate touchstone of the Fourth Amendment is reasonableness." *Id.* (internal quotation marks omitted). "One well-recognized exception applies when the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." *Id.* at 460 (internal quotation marks omitted). One such exigency is "the need to prevent the imminent destruction of evidence." *Id.* (internal quotation marks omitted).

The NIT search of Defendant's computer—a search inside his home—without a warrant issued in South Carolina was justified by the need to preserve fleeting evidence. Although Defendant obscured his identity and location, his crime—accessing child pornography on Playpen—occurred in the plain view of the FBI. The Fourth Amendment does not leave law enforcement helpless to trace criminal computer use occurring in plain view. Courts routinely allow warrantless seizures of laptop computers and other digital media containing child pornography under the exigent circumstances doctrine, because of "the fragile and easily destructible nature of the digital evidence at issue." *United States v. Blood*, 429 F. App'x 670, 671 (9th Cir. 2011); *see also, e.g.*, *United States v. Brown*, 701 F.3d 120, 127 (4th Cir. 2012); *United States v. Bradley*, 488 F. App'x 99, 105 (6th Cir. 2012); *United States v. Clutter*, 674 F.3d 980, 985 (8th Cir. 2012); *United States v. Diaz*, 435 F. App'x 329, 332 (5th Cir. 2011); *United States v. Vallimont*, 378 F. App'x 972, 974 (11th Cir. 2010). Because Defendant used sophisticated encryption software, the NIT was the only available means to locate him. Because the information collected by the NIT is evanescent, the FBI could learn his location (and from that his identity) only by deploying the NIT at the moment Defendant committed his crime. Even if Defendant's activities on Playpen somehow gave cause to believe Defendant was somewhere in South Carolina, there would have been no time to obtain a warrant in South Carolina. *See* Government's Motion for Reconsideration 18, *Levin*, Crim. No. 15-10271 (May 13, 2016), Dkt. No. 86 ("The information the NIT collected was also fleeting. If law enforcement had not collected IP addresses at the time of user communications with [Playpen], then, due to the site's use of Tor, law enforcement would have been unable to collect identifying information."). In other words, even if FBI agents had learned something that made their reliance on the warrant outside of the Eastern District of Virginia unreasonable, exigent circumstances nonetheless would have justified use of the NIT outside that district.[7]

5. The Government Did Not Intentionally Disregard Rule 41

Defendant argues "the [FBI] acted in intentional and deliberate disregard of Rule 41." (Dkt. No. 47 at 14.) Even though the violation of Rule 41 is a non-constitutional, suppression nonetheless would be appropriate if the violation arose from intentional disregard of the rule. *Simons*, 206 F.3d at 403. The Court however finds no intentional disregard of Rule 41. Special Agent Macfarlane was completely candid with the issuing magistrate judge about the method and scope of the NIT. He has testified that he knew the NIT would search computers outside the Eastern District of Virginia, and that he believed Rule 41(b)(4) authorized the warrant. Hr'g Tr. 62:23–25, 64:24–65:20, *Matish*, 4:16-16, Dkt. No. 61. Although the Court concludes his interpretation of Rule 41(b)(4) is incorrect, Agent Macfarlane's contrary view was not

[7] The *Darby* court summarily discounted the Government's assertion of the exigent circumstances doctrine because the Government had time to obtain a warrant in Virginia. 2016 WL 3189703, at *13 n.8. This Court disagrees with that reasoning. Playpen came online in August 2014. (Dkt. No. 58-1 ¶ 3.) A foreign nation informed the FBI that Playpen was in the United States in December 2014. (Dkt. No. 47-2 ¶ 38.) The FBI seized the server hardware and relocated it to Virginia in January 2015. (*Id.*) It seized administrative control of Playpen on February 19, 2015. (*Id.* ¶ 52.) It presented one hundred affidavit pages to obtain the warrant and Title III order on February 20, 2015. (Dkt. Nos. 47-2 & 47-3.) It used the NIT to identify Playpen users from February 20, 2015 to March 4, 2015. (Dkt. No. 47 at 1.) There was not time to obtain a search warrant in all 94 judicial districts.

unreasonable. *See, e.g.*, *Adams*, 2016 WL 4212079, at *6 ("The Government offers a tempting interpretation of this rule by comparing the placement of the NIT onto the government-controlled Playpen server to the concealment of a tracking device in a container holding contraband which is then tracked outside of the district where the warrant was issued."); *Acevedo-Lemus*, 2016 WL 4208436, at *7 ("It is not a stretch to say that the NIT functioned as a permissible 'tracking device' attached to child pornography that was subsequently downloaded by Defendant when his computer sent a request to the Playpen server."); *Matish*, 2016 WL 3545776, at *17 (concluding Rule 41(b)(4) permits the NIT search warrant); *Darby*, 2016 WL 3189703, at *12 (same); *Michaud*, 2016 WL 337263, at *6 ("The Court must conclude that the NIT Warrant did technically violate Rule 41(b), although the arguments to the contrary [regarding (b)(4)] are not unreasonable and do not strain credulity.")

Defendant also argues the Southern District of Texas's decision in *In re Warrant to Search a Target Computer at Premises Unknown* put the Government on notice that the NIT search warrant would violate Rule 41. *See* 958 F. Supp. 2d 753 (S.D. Tex. 2013). In that case, a Houston magistrate judge denied the Government's application for a warrant to use an NIT similar to the one at issue here in a bank fraud investigation, finding, *inter alia*, the application did not satisfy any of Rule 41(b)'s territorial limits on a magistrate judge's authority to issue a warrant. *Id.* at 758. Defendant speculates, "It is unlikely that the Government was unaware of this when it filed its application." (Dkt. No. 47 at 15.)

Defendant misunderstands the holding of *In re Warrant*, which did not hold search warrants could never issue "where the location of the Target Computer is unknown." *Compare* (Dkt. No. 47 at 15) *with* 958 F. Supp. 2d at 761 ("The court finds that the Government's warrant request is not supported by the application presented. This is not to say that such a potent investigative technique could never be authorized under Rule 41.") Indeed, the Supreme Court has said search warrants can issue when the location of the place to be searched is unknown because it is the very information sought. *Karo*, 468 U.S. at 718.

Regardless, the decision of a magistrate judge in Texas on what was then a matter of first impression in any circuit obviously does not thereafter bind every court in the nation. *See In re Warrant*, 958 F. Supp. 2d at 756 n.2 ("This appears to be a matter of first impression in this (or any other) circuit."). The FBI reasonably believed Rule 41(b)(4) authorized the warrant requested, and it was entitled to submit its application to a judicial officer for a decision. The FBI does not act with "deliberate disregard" of the rules regarding the magistrate judge's authority when it makes a detailed and forthright application to her.

Finally, Defendant cites the pending amendment to Rule 41 (effective December 1, 2016), which will explicitly allow warrants such as the NIT search warrant, as an implicit statement that "no reasonable interpretation of any provision in Rule 41(b)" permits the NIT search warrant. (Dkt. No. 47 at 15–16.) As explained above, the Court agrees the NIT search warrant violates Rule 41(b). So, in this Court's view, the motive for amending Rule 41 to allow future NIT search warrants is the belief such search warrants are necessary and reasonable. (*See* Dkt. No. 47-5 at 2 (memorandum to the Supreme Court stating that the amendment to Rule 41 to allow "certain types of remove electronic searches" was approved by an 11-1 vote of the Advisory Committee and a unanimous vote of the Standing Committee).) This Court sees no colorable argument suggesting that amending Rule 41 to allow magistrate judges to issue NIT search warrants in the future means evidence discovered pursuant to such warrants issued in the past must be suppressed as deliberate disregard of the former rule. The purpose of suppressing evidence is to prevent *future* misconduct. *Cf. Davis*, 564 U.S. at 236–37 ("Exclusion is not a personal constitutional right, nor is it designed to redress the injury occasioned by an unconstitutional search. The rule's sole purpose, we have repeatedly held, is to deter future Fourth Amendment violations.").

6. Defendant Was Not Prejudiced

Suppression is appropriate if a non-constitutional violation of Rule 41 prejudices the defendant. *Simons*, 206 F.3d 392, 403. This requires a standard for "prejudice." Defendant, citing First Circuit authority, argues prejudice "means being subjected to a search that might not have occurred or would not have been so abrasive." (Dkt. No. 47 at 12 (citing *United States v. Burgos-Montes*, 786 F.3d 92, 109 (1st Cir. 2015).) The Court finds that standard overbroad. Any Rule 41 violation means "being subjected to a search that *might* not have occurred." The Third Circuit's standard for prejudice better accords with Fourth Circuit case law on prejudice: "Our Circuit defines prejudice 'in the sense that it offends concepts of fundamental fairness or due process.'" *Werdene*, 2016 WL 3002376, at *10 (quoting *United States v. Hall*, 505 F.2d 961, 964 (3d Cir. 1974)); *cf. Noble v. Barnett*, 24 F.3d 582, 586 (4th Cir. 1994) ("To demonstrate prejudice, a petitioner must show 'actual prejudice' amounting to a denial of fundamental fairness.") The Court concludes that, to show prejudice from the NIT search warrant's violation of Rule 41, Defendant must show the violation of Rule 41 offends fundamental fairness. Defendant totally fails to show that the conduct of the FBI in obtaining the NIT search warrant was in any way fundamentally unfair to persons deliberately concealing their locations while committing crimes.

But even under the lax standard Defendant proposes, there is no prejudice because the search could have occurred regardless. Probable cause is not at issue. Had the FBI sought NIT search warrants in every judicial district for computers accessing Playpen, the FBI would have obtained them.[8] *See Acevedo-Lemus*, 2016 WL 4208436, at *7 ("Nor was Defendant prejudiced by any potential Rule 41 violation. After all, the FBI could have [obtained warrants] in every judicial district in the country . . . ."). There is no genuine issue of scope or particularity—Defendant's argument is simply that the wrong magistrate judge issued the NIT search warrant. He does not attempt to explain how correction of that error could have benefited him. If the same NIT warrant application had been made to a South Carolina magistrate judge, the result, for Defendant, would have been the same.

Moreover, Rule 41(b) by its express terms applies only to magistrate judges. At least one court has concluded a district judge could have issued the NIT search warrant. *Levin*, 2016 WL 2596010, at *14 ("With respect to district judges, neither Rule 41(b) nor Section 636(a) of the Federal Magistrates Act restricts their inherent authority to issue warrants consistent with the Fourth Amendment."). The circuits are split on whether Rule 41(b) applies to district judges. The First, Third, Fifth, and D.C. Circuits have indicated Rule 41(b) does limit the authority of district judges. *See United States v. Golson*, 743 F.3d 44, 51 (3d Cir. 2014) ("Rule 41(b) grants the authority to issue search warrants to federal judges . . . ."); *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding a warrant issued by a district judge to search property outside that judge's district violated Rule 41(b)(2)); *United States v. Brouillette*, 478 F.2d 1171, 1175 (5th Cir. 1973) ("The basis for the issuance of any federal search warrant is Rule 41 . . . ."); *see also United States v. Krawiec*, 627 F.2d 577, 580 (1st Cir. 1980) (citing *Brouillette* with approval). The Second and Seventh Circuits hold "Rule 41 does not define the extent of the court's power to issue a search warrant." *United States v. Villegas*, 899 F.2d 1324, 1334 (2d Cir. 1990); *United States v.*

[8] That the FBI did not actually have time to seek a warrant in every district is an exigent circumstance cutting against Defendant's argument for suppression.

Torres, 751 F.2d 875, 878 (7th Cir. 1984) ("[T]he power to issue a search warrant was historically, and is still today, an inherent (by which we mean simply a nonstatutory, or common law) power of a court of general jurisdiction.").[9]

The Seventh Circuit provides the most extensive analysis of district courts' inherent power to issue search warrants. The *Torres* court cited English precedent extending from the twelfth century to establish the authority to issue search warrants as "an aspect of the court's power to regulate procedure." 751 F.2d at 878. Turning to American precedent, it concluded,

> The power to issue a search warrant is a common law power in America as well as England, *see Adams v. New York*, 192 U.S. 585, 598 (1904); *Boyd v. United States*, *supra*, 116 U.S. at 623 [1886]; *United States v. Maresca*, 266 Fed. 713, 721 (S.D.N.Y. 1920) (Hough, J.), and in the federal system as well as in the states. While "the whole criminal jurisdiction of the courts of the United States [is] derived from Acts of Congress," *Jones v. United States*, 137 U.S. 202, 211 (1890), this does not mean that every procedural incident of their jurisdiction is statutory. Until 1917 there was no general statutory authorization for the issuance of federal search warrants . . . .

Id. at 879 (parallel citations omitted). The Second Circuit has adopted similar reasoning.

> First, we note that Rule 41 does not define the extent of the court's power to issue a search warrant. Obviously the Fourth Amendment long antedated the Federal Rules of Criminal Procedure, which were first adopted in 1944. Given the Fourth Amendment's warrant requirements, and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met.

[9] The forthcoming amendment to Rule 41(b) changes the subsection's caption from "Authority to Issue a Warrant" to "Venue for a Warrant Application." (Dkt. No. 47-5 at 9.) Possibly that could be taken to mean the rule should apply to all search warrants. The committee comments regarding the caption change state "the word 'venue' makes clear that Rule 41(b) identifies the courts that may consider an application for a warrant, not the constitutional requirements for the issuance of a warrant." (*Id.* at 32.) The committee notes evidence no discussion of the inherent power of Article III judges versus the statutory power of magistrate judges. If the revision meant to limit the inherent powers of district courts, a more logical way to express that intent would have been to revise the references to magistrate judges. Instead, another reference to magistrate judges was added. (*Id.* at 9.) Moreover, even if the revised caption is construed to limit the inherent power of district courts, replacement of "authority" with "venue" undercuts any argument that a violation of Rule 41(b) could be constitutional in nature.

Villegas, 899 F.2d at 1334.

This Court concludes that, upon a showing of probable cause that a crime has occurred within his district, a federal district judge has territorial jurisdiction to issue a search warrant to discover the location of the perpetrator. Jurisdiction is not vitiated *post facto* when the search warrant's execution reveals the perpetrator was located outside the district. Were that the case, the Supreme Court's allowance of search warrants to discover the location of a place to be searched would be nearly meaningless. *Cf. Karo*, 468 U.S. at 718. Although the Court agrees with Defendant's arguments that "[i]t is not for this Court to rewrite [Rule 41] to keep up with new technological developments" and that "[i]t is for the United States Congress to address any shortcomings in [Rule 41]" insofar as they apply to the statutory authority of magistrate judges, the Court cannot accept them insofar as they imply the Court has no common law power to issue search warrants not specifically authorized by some codified rule of procedure. "The motto of the Prussian state—that everything which is not permitted is forbidden—is not a helpful guide to statutory interpretation." *Torres*, 751 F.2d at 880. Indeed, the argument that a court cannot issue a search warrant unless authorized by a codified rule is best made in a civil law jurisdiction. This is a common law jurisdiction, and "[i]t has been said so often as to have become axiomatic that the common law is not immutable but flexible, and by its own principles adapts itself to varying conditions." *Funk v. United States*, 290 U.S. 371, 383 (1933).

The conclusion that the procedural defect in the NIT search warrant would have been cured simply by having a district judge sign the warrant reduces the Rule 41 violation in this case to the most trivial of procedural defects. Four district judges and three senior judges sit routinely in the Alexandria courthouse. *Levin*, 2016 WL 2596010, at *14. One of those district judges, the Honorable Anthony Trenga, signed the Title III order in this case. (*See* Dkt. No. 47-2 at 61.)

Defendant was in no way prejudiced by a magistrate judge signing the NIT search warrant instead of Judge Trenga, in the same building on the same day that Judge Trenga signed the corresponding Title III order.

Finally, the Court finds even if Defendant were prejudiced by a Virginia magistrate judge, rather than some other judicial officer (such as a Virginia district judge), issuing the NIT search warrant, he would be estopped from asserting that prejudice because he caused it. A person cannot use sophisticated software to conceal the location of his computer and then challenge a search warrant on the basis that the Government could not determine the exact location of his computer. This appears to be a question of first impression, and the Court does not suggest a defendant may be estopped on the issue of guilt or innocence. But suppression is collateral issue. Criminal defendants may be estopped on collateral issues, and, more specifically, they may be estopped from challenging search warrants. *See, e.g.*, *Kokoski v. Keller*, Civ. No. 5:06-730, 2007 WL 2471290, at *11 (S.D.W. Va. Aug. 30, 2007) (noting "Plaintiff was estopped from challenging the validity of the search warrant, in light of his guilty plea").[10]

Nor does the Court suggest that deliberately concealing the location of one's computer estops the assertion of Fourth Amendment rights. To be sure, the act of hiding does not obviate the constitutional requirement for a search warrant, supported by probable cause. But Defendant does not challenge the probable cause supporting the NIT search warrant, nor does he challenge the neutrality of the magistrate judge, nor does he challenge NIT search warrant's scope or

[10] Typically, an estoppel of a defendant in a criminal context means some form of issue preclusion—the avoidance of relitigation. "[C]ourts have held that the doctrine of collateral estoppel can be used to prevent a criminal defendant from relitigating the lawfulness of searches and seizures." *United States v. Yung*, 786 F.Supp. 1561, 1565 (D. Kan. 1992). Given that a defendant can be estopped from relitigating a valid constitutional issue, it seems reasonable that a defendant can be estopped from litigating a non-constitutional procedural issue that he caused.

particularity, except to argue it was insufficiently particular because specified the Virginia-based server as the search location instead of Defendant's own computer, which just repeats his argument that the wrong magistrate judge issued the warrant. The warrant issued in Virginia rather than South Carolina because of Defendant's substantial efforts to conceal his location while committing federal crimes. As a result, those crimes were visible to authorities in Virginia but not to authorities in South Carolina. A defendant may be estopped from asserting a procedural rule against the Government—even if the issue is collateral to a criminal matter—if the defendant *caused* the violation despite the Government's best efforts, undertaken in good faith, to avoid the violation. *See Union Mut. Ins. Co. v. Wilkinson*, 80 U.S. 222, 233 (1871) ("And although the cases to which this principle is to be applied are not as well defined as could be wished, the general doctrine is well understood and is applied by courts of law as well as equity where the technical advantage thus obtained is set up and relied on to defeat the ends of justice . . . .").

Estoppel is "[a] bar that prevents one from asserting a claim or right that contradicts what one has said or done before." Estoppel, Black's Law Dictionary (10th ed. 2014). Defendant's use of Defense Department encryption software to hide his location while accessing child pornography meant the Government could know only the location of the child pornography accessed—Virginia—and so caused FBI agents to seek a warrant in Virginia for information regarding Defendant's location. Defendant now moves to suppress evidence on the basis that the Government sought a warrant in Virginia. In other words, Defendant's deliberate deeds made it impossible for a search warrant to issue from any jurisdiction other than the jurisdiction where Playpen was located. He cannot now argue he is prejudiced by the issuance of a search warrant from the jurisdiction where Playpen was located. Because his misconduct caused the procedural error he complains of, his complaint is estopped by "the equitable maxim that no party should be permitted to take advantage of its own wrongs." *K. Bell & Associates, Inc. v. Lloyd's Underwriters*, 827 F. Supp. 985, 989 (S.D.N.Y. 1993).

IV. Conclusion

For the foregoing reasons, the Court **DENIES** the motion to suppress (Dkt. No. 47).

AND IT IS SO ORDERED.

Richard Mark Gergel
United States District Court Judge

September 14, 2016
Charleston, South Carolina